10/686,773
10/688,499

AMENDMENTS TO THE SPECIFICATION

NM 8/12/04 On page 6, paragraph **[0017]**, please amend as follows:

[0017] Various embodiments of the present invention may be provided as a computer program product, which may include a machine-readable medium having stored thereon instructions, which may be used to program a computer (or other electronic devices) to perform a process according to various embodiments of the present invention. ~~The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs, magneto-optical disks, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, flash memory, or another type of media/machine-readable medium suitable for storing electronic instructions.~~ The machine-readable medium may include, but is not limited to, a floppy diskette, an optical disk, a Compact Disk-Read Only Memory (CD-ROM), a magneto-optical disk, a Read Only Memory (ROM), a Random Access Memory (RAM), an Erasable Programmable ROM (EPROM), an Electrically EPROM (EEPROM), a magnetic or optical card, a flash memory, or another type of media/machine-readable medium suitable for storing electronic instructions. Moreover, various embodiments of the present invention may also be downloaded as a computer program product, wherein the program may be transferred from a remote computer to a requesting computer by way of data signals embodied in a carrier wave or other propagation medium via a communication link (e.g., a modem or network connection).

~~10186753~~
10688499

to one embodiment, the process of attestation may be used for having the signed value reported to a remote system via, for example, a cryptographic protocol. The remote system may ascertain the trustworthiness of the measured software and may make a trust decision based on the trustworthiness of information reported by the hardware TCB 206 of the measured system 100.

On page 20, paragraph **[0049]**, please amend as follows:

[0049] Figure 5 is a block diagram illustrating an embodiment of a horizontally extended Trusted Computing Base. According to one embodiment, as described with ~~referenced~~ reference to Figures 2 and 3, a Trusted Platform Module (TPM) 204 and other trustworthy hardware components (e.g., hardware-based measurement of booted software and Direct Memory Access (DMA) protection from input/output (I/O) devices) may be used to form a trustworthy hardware computing base, such as Level one tamper-resistant hardware Trusted Computing Base (L1 TCB) 206. According to one embodiment, the L1 TCB 206 may be extended horizontally into a horizontally extended TCB 500.

NM 8/24/01 On page ~~23~~ 22, paragraph **[0053]**, please amend as follows:

[0053] According to one embodiment, the software-based L2 TCB 502 may not merely virtualize the functionality of the hardware-based L1 TCB 206, but also perform the virtualization such that the trust and security properties of the hardware-based L1 TCB 206 may be mimicked or imitated in software of the L2 TCB 502. According to one embodiment, the mimicking of the trust and security properties of the L1 TCB 206 may be necessary for a software TCB layer, such as the L2 TCB 502, to represent its own